UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

| APPLICATION NO. | FILING DATE | FIRST NAMED INVENTOR | ATTORNEY DOCKET NO. | CONFIRMATION NO. |
|---|---|---|---|---|
| 10/749,502 | 12/31/2003 | Soo-Hyung Lee | 51876P585 | 1208 |

8791 7590 10/01/2007
BLAKELY SOKOLOFF TAYLOR & ZAFMAN
1279 OAKMEAD PARKWAY
SUNNYVALE, CA 94085-4040

| EXAMINER | |
|---|---|
| NOORISTANY, SULAIMAN | |

| ART UNIT | PAPER NUMBER |
|---|---|
| 2146 | |

| MAIL DATE | DELIVERY MODE |
|---|---|
| 10/01/2007 | PAPER |

**Please find below and/or attached an Office communication concerning this application or proceeding.**

The time period for reply, if any, is set in the attached communication.

5

| Office Action Summary | Application No.<br>10/749,502 | Applicant(s)<br>LEE ET AL. | |
|---|---|---|---|
| | Examiner<br>Sulaiman Nooristany | Art Unit<br>2109 | |

*-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --*

## Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

## Status

1)□ Responsive to communication(s) filed on _____.

2a)□ This action is **FINAL**. 2b)☒ This action is non-final.

3)□ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

## Disposition of Claims

4)☒ Claim(s) *1-4* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)□ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-4* is/are rejected.

7)□ Claim(s) _____ is/are objected to.

8)□ Claim(s) _____ are subject to restriction and/or election requirement.

## Application Papers

9)□ The specification is objected to by the Examiner.

10)□ The drawing(s) filed on _____ is/are: a)☒ accepted or b)□ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)□ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

## Priority under 35 U.S.C. § 119

12)☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☒ All b)□ Some * c)□ None of:

1.☒ Certified copies of the priority documents have been received.

2.□ Certified copies of the priority documents have been received in Application No. _____.

3.□ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

**Attachment(s)**

1) ☒ Notice of References Cited (PTO-892)

2) □ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3) ☒ Information Disclosure Statement(s) (PTO/SB/08)
Paper No(s)/Mail Date *12/31/2003 & 11/25/2005*.

4) □ Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____ .

5) □ Notice of Informal Patent Application

6) □ Other: _____.

## *Detailed Action*

This Office Action is response to the application (10749502) filed on 31 December 2003.

## *Claim Rejections - 35 USC § 112*

The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter, which the applicant regards as his invention.

**Claims 1-4** are rejected under 112, second paragraph as being indefinite for failing to particularly point and distinctly claim the subject matter which applicant regards as the invention

A. The following terms lack proper antecedent basis:

**As per claim 1**, line 6, it is unclear if "*a network level*" refers to "the network level" in lines 1-2 [i.e. if they are the same terms such as " the network level" or "said network level" should be used. However, appropriate correction is required.

**As per claim 4**, line 7, it is unclear if "*a network level*" refers to "the network level" in lines 3 [i.e. if they are the same terms such as " the network level" or "said network level" should be used. However, appropriate correction is required.

B. The claim language I the following claims is not clearly understood:

**As per claim 1**, line 15, it is not clearly indicated whether "*seriousness* of abnormal traffic" is the same as "error, threshold level".

**As per claim 4**, line 16, it is not clearly indicated whether "*seriousness* of abnormal traffic" is the same as " data errors, threshold level of data".

### *Claim Rejections - 35 USC § 102*

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless-
>
> (e) the invention was described in-
> (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent; or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, *except* that an international application filed under the treaty defined in section 351(a) shall have the effects for the purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English.

**Claims 1-4** are rejected under 35 U.S.C. 102(e) as being anticipated by **Porras et al.** U.S. Patent Application Publication No. **US 2003/0212903.**

**Regarding claim 1**, Porras teaches wherein a method for detecting abnormal traffic at the network level using a statistical analysis, the method comprising the steps of:

a) gathering local traffic data from each network device and integrating a plurality of the local traffic data to generate traffic data in a network level (**Fig. 1, unit 12a –12c indicating the integrated of different domains in a network**);

b) extracting a characteristic traffic data based on the traffic data in the network level (**characteristic data forms from the header of the packet [0032]**);

c) comparing the characteristic traffic data with a characteristic traffic data profile resulting from statistical computations (**Fig. 5, unit 78 (compare one of the short-term profiles to a corresponding long-term statistical profile)**, and determining whether there is abnormal traffic in the network (**Fig. 4, unit 70 (Determine if statistical profile is abnormal**); and

d) updating the characteristic traffic data profile using the characteristic traffic data if there is no abnormal traffic in the network, analyzing seriousness of the abnormal traffic and monitoring the abnormal traffic if there is abnormal traffic in the network (**the monitor can respond by reporting (updating) the activity (i.e. seriousness of the abnormal traffic like privilege network errors and abnormal levels of the network level) to another monitor or by executing a countermeasure response [0071]**).

**Regarding claim 2**, Porras taught the method in claim 1, as described above. Porras further teaches wherein the characteristic traffic data includes:

information on traffic assigned to an application port which is selected according to an application service (**TCP port identifier [0036]**);

information on traffic of which packet size is identical (**network measures number of packets and number of kilobytes [0037]**); and

information on traffic of which the number of source-destination pairs, which represents the number of source addresses of the traffic having the same target address (**categorical measures including the network source and destination address [0036], packet source addresses and destination addresses match is**

**given internal host [0033]**).

**Regarding claim 3**, Porras taught the method in claim 1, as described above. Porras further teaches wherein e) transmitting the analysis result of the seriousness of the abnormal traffic to an abnormal traffic processing system **(the overall volume of discarded packets as well as a measure analyzing the disposition of the discarded packets (abnormal packet) can provide insight into unintentionally malformed packets resulting from poor line quality or internal errors in neighboring hosts [0076]**).

**Regarding claim 4**, Porras teaches wherein a computer-readable recording medium for storing a program that implements a method for detecting abnormal traffic at the network level using a statistical analysis (**Fig. 6 computer**), the method comprising the steps of:

a) gathering local traffic data from each network device and integrating a plurality of the local traffic data to generate traffic data in a network level (**Fig. 1, unit 12a –12c indication of integrated of different domains in a network**);

b) extracting a characteristic traffic data based on the traffic data in the network level (**characteristic could be formed from the header [0032]**);;

c) comparing the characteristic traffic data with a characteristic traffic data profile resulting from statistical computations (**Fig. 5, unit 78 (compare one of the short-term profiles to a corresponding long-term statistical profile)**, and determining whether there is abnormal traffic in the network (**Fig. 4, unit 70 (Determine if statistical profile is abnormal**); and

d) updating the characteristic traffic data profile using the characteristic traffic data if there is no abnormal traffic in the network, analyzing seriousness of the abnormal traffic and monitoring the abnormal traffic if there is abnormal traffic in the network (**Based on this comparison, the monitor can respond by reporting (updating) the activity (i.e. seriousness of the abnormal traffic like privilege network errors and abnormal levels of the network level) to another monitor or by executing a countermeasure response [0071]**).

### *Conclusion*

The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

US Patent 6,279,037 B1 to Tams et al.
US Patent 6,738,811 B1 to Liang, Charles
US Patent App. 2002/0131369 A1 to Hasegawa et al.
US Patent App. 2003/0115483 A1 to Liang, Yung Chang
US Patent App. 2004/0225877 A1 to Huang, Zezhen
US Patent App. 2005/0108377 A1 to Lee et al.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Sulaiman Nooristany whose telephone number is (571) 270-1929. The examiner can normally be reached on M-F from 9 to 5. If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Jeff Pwu, can be reached on (571) 272-6798. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300. Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Sulaiman Nooristany 9/6/2007

Supervisory Patent Exmr.